UNITED STATES MARINE CORPS
Marine Corps Recruit Depot/Western Recruiting Region
1600 Henderson Avenue Suite 235
San Diego, California 92140-5001

IN REPLY REFER TO:
DepO P5230.1A
5E
OCT 0 4 2001

DEPOT ORDER P5230.1A

From: Commanding General
To: Distribution List

Subj: STANDING OPERATING PROCEDURES FOR COMMUNICATIONS AND INFORMATION SYSTEMS DEPARTMENT (SHORT TITLE: CISD SOP)

Ref: (a) DODINST 5200.1 (NOTAL)
(b) SECNAVINST 5239.3 (NOTAL)
(c) OPNAVINST 2201.2 (NOTAL)
(d) OPNAVINST 5230.24 (NOTAL)
(e) NAVSO P5239-04 (NOTAL)
(f) NAVSO P5239-07 (NOTAL)
(g) NAVSO P5239-08 (NOTAL)
(h) NAVSO P5239-29 (NOTAL)
(i) IRM 5239-08 (NOTAL)
(j) IRM 5239-10 (NOTAL)
(k) DEP0 5239.4 (NOTAL)

Encl: (1) Locator Sheet

1. Purpose. To establish policy and procedures governing the acquisition, security, use, accountability, and management of end-user computing equipment (EUCE), primarily microcomputers, network servers, and associated peripherals, to include telephone and radio communications equipment.

2. Cancellation. DepO P5230.1

3. Background. In compliance with references (a) through (k), this SOP provides guidance for the employment of EUCE and communications assets within this Command. It applies to all users of computing and communcations assets and facilities at the Marine Corps Recruit Depot, San Diego, California. The contents of this SOP are unclassified to permit the widest possible dissemination.

4. Recommendation. Recommendations concerning the contents of SOP are invited. Such recommendations will be forwarded to the Director, Communications and Information Systems Department (Attn: Director, Communications and Information Systems Support Division) via the appropriate chain of command.

5. Certification. Reviewed and approved this date.

T. W. SPENCER
Chief of Staff

DISTRIBUTION: A

LOCATOR SHEET

Subj: STANDING OPERATING PROCEDURES (SOP) FOR COMMUNICATIONS AND INFORMATION SYSTEMS DEPARTMENT (CISD)

Location: _____
(Indicate location(s) of copy(ies) of this Manual.)

CISD SOP

RECORD OF CHANGES

Log completed change action as indicated.

Change Number	Date of Change	Date Entered	Signature of Person Incorporating Change

CISD SOP

CONTENTS

This page is intentionally left blank.

CISD SOP

CHAPTER 1

ORGANIZATION

FIGURE

This page is intentionally left blank.

CHAPTER 1

ORGANIZATION

1000. GENERAL. The Communications and Information Systems Department (CISD) at Marine Corps Recruit Depot (MCRD), San Diego, is an integral part of the Command and plays an important role in the support of the Depot's mission. Functional areas requiring diligent attention include fiscal status, acquisition, accountability, security, and maintenance of existing voice and data communications systems, Automated Information System (AIS) systems, End-User Computing Equipment (EUCE) systems, Local Area Network (LAN) systems, and Internet Access.

1001. ORGANIZATION

1. CISD is assigned the mission of installing, operating, providing security for, and maintaining high speed, reliable voice and data communications in support of the recruiting and recruit training efforts aboard MCRD, San Diego. Tasking includes planning, budgeting, coordinating, interpreting and implementing voice and data communications, AIS, EUCE, and LAN systems aboard MCRD.

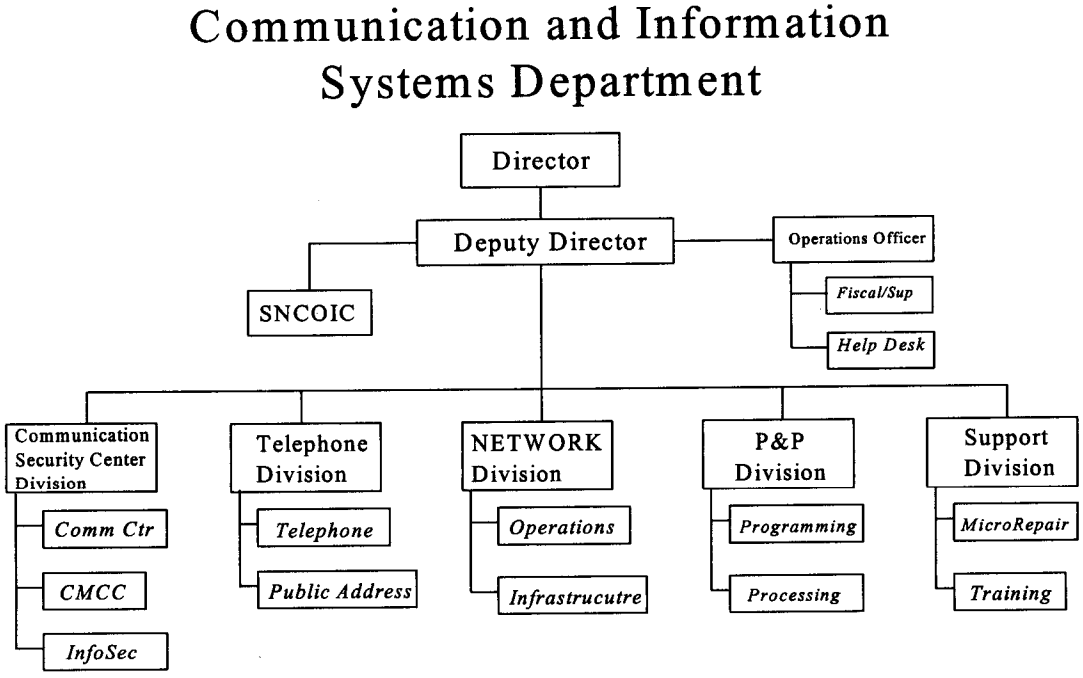

Figure 1-1. CISD Functional Organization

2. CISD is organized into six functional areas (see Figure 1). The Director, CISD, functions as a General Staff Officer and exercises staff cognizance over the following subordinate functional areas:

a. CISD Operations Support Center

b. Communications-Security Center Division

c. Telephone Division

d. Network Division

e. Programming and Processing Support Division

f. Information Systems Support Division (ISSD)

3. The functions of each functional area are critical to the successful operation of CISD.

a. CISD Operations Support Center. Executes the overall policies and procedures, as well as coordinates the fiscal, supply, inventory, administrative, and service operations of the department.

b. Communication-Security Center Division. Manages and maintains operational support for the Electronic Messaging Systems and all of its resources, as well as maintains the Depot's Information Systems Security (INFOSEC) program to ensure all regulations are being met. Additionally, they maintain overall cognizance for the Classified Material Control Center, to include the Communications Security (COMSEC) Material System.

b. Telephone Division. Manages and supports the Depot in all areas of telephone and public address, to include all resources and equipment. They also oversee the telecommunications support and setup of the Emergency Operations Center.

c. Network Division. Manages the Depot's data communications systems and associated equipment and cabling. Functions include the LAN, network applications, Internet and external data communications support.

d. Programming and Processing Support Division. Coordinates local software development and processing requirements. They also provide production job processing and printing for Depot customers.

f. ISSD. Coordinates and implements procedures governing acquisition, accountability, use, management, and maintenance of Depot communications and end-user computing assets.

1002. RESPONSIBILITIES OF THE DIRECTOR, CISD. The Director, CISD is responsible to the Commanding General for:

1. Carrying out duties as the Departmental General Staff Officer.

2. Acting as the cognizant officer for all voice and data communications, EUCE, and LAN systems matters that require action by the Command.

3. Advising the Commanding General, via the Chief of Staff, on matters pertaining to voice and data communications, AIS, EUCE, and LAN systems support and the state of technology aboard the Depot.

4. Advising and assisting other officers in the continuing effort to

improve voice and data communications, AIS, EUCE, and LAN systems and practices aboard MCRD.

5. Overseeing routine and special voice and data communications, AIS, EUCE, and LAN systems operations within MCRD to ensure optimum operational readiness at all times.

6. Acting as the Designated Approving Authority (DAA) and ensuring compliance with the Department of the Navy INFOSEC program for the Depot. This includes the security and the accreditation of the data systems.

7. Directing an adequate continuous training program, both in military occupational specialty (MOS) training and mission-oriented training, for CISD personnel to stay on the cutting edge of voice and data communications, AIS, EUCE, and LAN in systems technology.

8. Recommending appropriate policy and procedures in matters pertaining to the effective and efficient deployment of voice and data communications, AIS, EUCE, and LAN systems technology.

1003. CISD OPERATIONS SUPPORT CENTER

1. General. The CISD Operations Support Center executes the policies and procedures established by the Director, CISD, pertaining to the operation of fiscal, supply, inventory, administrative, and service requirements of the department.

2. Organization

a. The CISD Operations Support Center coordinates the daily operation of CISD. Priority functions include efficient, effective, and fiscally responsible planning for valid communications and computing assets and the timely implementation of those plans.

b. The CISD Operations Support Center is headed by the Operations Officer and is organized into four sections. The Operations Officer exercises staff cognizance over the following subordinate sections:

(1) Staff Non-commissioned Officer-in-charge (SNCOIC)

(2) Supply/Inventory Section

(3) Fiscal Section

(4) Customer Helpdesk

3. The functions of each section are critical to the successful operation of CISD Operations Support Center.

a. SNCOIC. The SNCOIC maintains liaison between CISD and Headquarters Company, Headquarters and Support Battalion on military matters. Advises the Director, CISD, and the Operations Officer on military and enlisted matters. Assists in the execution of policies, procedures, and plans for the department. Coordinates the maintenance, policing, and general upkeep of CISD facilities.

b. Supply/Inventory Section. The Supply/Inventory Section maintains a database of all EUCE and telephone assets for the Depot to include assigned and unassigned assets. Submits procurement documents for computing, networking and communications assets, verifies incoming shipments, and signs for procurements of these assets. Prepares and submits work requests and/or material requests for EUCE/communications assets. They are also responsible to maintain a Responsible Individual/Information Systems Coordinator (RI/ISC) for each unit where EUCE/Communications material is issued.

c. Fiscal Section. The Fiscal Section manages Fund Administrator's account 1A for CISD, to include verifying and submitting invoices for maintenance contract payments. Maintains and reconciles desktop ledgers for fiscal transactions. Maintains correspondence and directives for the CISD fiscal cost center. Separates, audits, and verifies telephone billings for the Depot.

d. CISD Help Desk. The Help Desk provides a centralized point of contact for responsive support within the Depot while increasing customer self-sufficiency. To guarantee the highest level of customer satisfaction, Help Desk Support personnel will strive to handle all trouble calls promptly, courteously, and with dispatch, resolve or refer the program to the appropriate technical section immediately.

3. Responsibilities. The CISD Operations Support Center is responsible for:

a. The day-to-day oversight of the CISD Operations Support Center.

b. The scheduling of CISD personnel to meet administrative requirements and military quotas.

c. Liaison with units external to the department in matters pertaining to CISD support services.

d. The effective planning of CISD budget.

e. The efficient management of the CISD cost center.

f. The effective coordination of MOS and mission-oriented training of CISD personnel.

1004. PROGRAMMING AND PROCESSING SUPPORT DIVISION

1. General. The Programming and Processing Division executes the policies and procedures established by the Director, CISD, pertaining to the local software development and processing requirements.

2. Organization

a. The Programming and Processing Division coordinates local software development, database management, and processing requirements. The Division provides custom software development, mission critical database management, production job processing, and print for Depot customers. Priority functions include an active role in effectively incorporating automated technology on a Depot-wide level. Conducts Needs Assessments Studies to validate requests for application and production development and determines the appropriate

platforms necessary to meet the customer's requirements.

b. The Division is headed by the Director, Programming and Processing Division, and is organized into two branches:

(1) Programming Branch

(2) Processing Branch

3. The functions of each are critical to the successful operation of the Programming and Processing Support Division.

a. Programming Branch. Programming Branch provides programming for computer languages supported aboard MCRD, San Diego. Code modules are designed and documented by the Project Team Leaders and/or Programming Analyst. The Branch also generates documentation for all modules coded.

b. Processing Branch. Processing Branch ensures the accessibility and reliability of data for mission critical Class I and Class II applications used by MCRD San Diego / Western Recruiting Region. In addition the Processing Branch schedules, processes, and prints all production jobs in accordance with established guidelines. The Branch also provides maintenance of JCL and mainframe datasets, and a link between the Depot customers and other Data Processing organizations in the implementation and maintenance of Class 1 and Class 2 mainframe programs.

4. Responsibilities. The Programming and Processing Support Division is responsible for the timely and appropriate execution of the following functions:

a. The management of mainframe and network data processing support on the Depot. This includes:

(1) Class I Mainframe Data Processing. The Processing Branch is the official liaison between the customer and all Class I processing sites (Camp Pendleton and St. Louis.) The Programming Branch acts as the official liaison between the customer and all Class I development sites.

(2) Class II Mainframe Data Processing, System Development, and System Maintenance. Processing Branch ensures reliable functioning of scheduled applications and Processing makes modifications to the run-time environment to suit specific needs of the customer to include the restructuring and assignment of input/output data. Programming makes modifications to the output reports and internal utilities for these mainframe jobs.

b. Networked, Multi-User Applications. Processing ensures data integrity of accepted mission critical databases. Processing ensures that data backups (generations) are created to an agreed schedule. Programming writes applications that provide data entry screens, views, and reports from those centralized data pools.

1005. NETWORK DIVISION

1. General. The Network Division executes the policies and procedures handed down by the Director, CISD, pertaining to the coordination and implementation procedures governing the management of the Depot's data communications systems.

2. Organization

a. The Division, under the cognizance of the Director, CISD, is assigned the mission of providing support services appropriate to the efficient and effective administration and management of Depot LAN support and resources, and the input/output of data processing and data connections of the Marine Corps Enterprise Network (MCEN).

b. The Division is headed by the Director, Network Division. The Director exercises staff cognizance over the Network Division.

c. The functions of the Division are critical to the successful operation of the Network Division.

d. The LAN Branch plans, installs, manages, and maintains Depot LAN hardware support and resources. The Branch also administers Depot LAN and network resources, including standards management, acquisitions, and configuration management.

3. Responsibilities. The Network Division is responsible for the timely and appropriate execution of the following functions:

a. The management of the LAN resources of the Depot.

(1) Maintains a current inventory of all LAN and computer network resources, as well as the structure and layout.

(2) Supports all official requirements and standards concerning EUCE in general, and LAN and computer networking in particular.

(3) Coordinates MCEN operations issues with the MITNOC, MCB Quantico, Va.

(4) Serve as technical representative for the Depot of the Defense Information System Agency on matters concerning external data communications.

(5) Serves as Depot representative to DoD and commercial agencies concerning data communications, network systems and inter-agency applications.

1006. INFORMATION SYSTEMS SUPPORT DIVISION

1. General. The ISSD executes the policies and procedures established by the Director, CISD, pertaining to the coordination and implementation procedures governing the acquisition, use, maintenance, and management of Depot communications and EUCE assets in accordance with established regulations.

2. Organization

a. The ISSD, under the cognizance of the Director, ISSD, is assigned the mission of providing support services appropriate for the efficient and effective utilization of Depot communications and EUCE assets. Priority functions include appropriate training support for end-users, validation of requirements and procurement recommendations for EUCE assets, and maintenance support for these assets.

b. The Division is headed by the Director, ISSD, and is organized into two branches:

(1) Maintenance Branch

(2) Training Branch

c. The functions of each are critical to the successful operation of the ISSD.

(1) Maintenance Branch. The Maintenance Branch provides preventive and corrective maintenance on all Depot EUCE assets, excluding the LAN equipment. The Branch also provides on-site assistance in response to trouble calls received from end-users.

(2) Training Branch. The Training Branch provides classroom and on-site training in the efficient and effective uses of EUCE assets. Courses provided include computer operating systems, supported application programs, and other performance enhancement courses. The staff of the Branch provides on-site assistance in response to requests received from end-users.

3. Responsibilities. The ISSD is responsible for the timely and appropriate execution of the following functions:

a. Analysis and validation of requests for EUCE computing assets, and approve specific equipment or system(s) to satisfy validated requirements.

b. Ensures that the proposed utilization of requested computing assets be justified in terms of manpower savings or increased productivity.

c. Prepares procurement package recommendations for all EUCE and associated peripherals, including software, for technical compliance with reference (a).

d. Recommends contract provisions covering leased equipment and assist in determining contractual maintenance coverage.

e. Coordinates training/information between EUCE vendors and users.

f. Provides maintenance on all nonproprietary EUCE.

1007. COMMUNICATIONS-SECURITY CENTER DIVISION

1. General. The Communications-Security Center Division executes policies and procedures endorsed by the Director, CISD, and in security matters under the direction of the DAA who has been appointed in writing by the Commanding General, MCRD, San Diego. The CISD Department Officer fills the DAA position. The Division manages and maintains operational support for the Defense Message System (DMS) and all of its resources, Depot's INFOSEC program to ensure all regulations are being met and the 3270 Mainframe access. It also maintains overall cognizance of the Classified Material Control Center (CMCC).

2. Organization. The Division is headed by the Director, Communications-Security Center Division and is organized into three branches:

a. INFOSEC Branch

b. DMS Local Control Center (LCC)

c. CMCC Branch

d. All of these branches are critical to the successful daily operations of the CISD, with daily responsibilities to the Depot.

3. Responsibilities

a. INFOSEC Branch implements and maintains the Activity Automated Information System Security Plan to protect the AIS resources against accidental or intentional destruction, unauthorized modification, disclosure of data, and unauthorized denial of service. Conducts periodic Security Surveys and implements the Risk Management Process to ensure AIS resources are safeguarded from these threats. Conducts Annual Information Assurance workshops for all Depot personnel. 3270 Access is headed by the Depot Terminal Area Security Officer (TASO) who manages the control and dissemination of user and system ID's and passwords, ensuring overall system security.

b. The LCC provides incoming and outgoing message communication processing to include receipt and distribution to the DMS, and conducts training classes on the Common Message Processing that is used for releasing of traffic to the DMS.

c. CMCC Branch receives, retains custody of, and distributes classified materials, plus those materials distributed by the Communications Security Material Systems, to include the custody and keying of the Secure Telephone Third Generation equipment.

1008. TELEPHONE DIVISION

1. General. The Telephone Division executes the policies and procedures handed down by the Director, CISD, pertaining to the coordination, implementation and procedures governing the management of the Depot's telephone network.

2. Organization

a. The Division, under the cognizance of the Director, CISD, is assigned the mission of providing reliable telephone and public address support for the Depot. Services provided by the Division include managing and maintaining the telephone network and providing reliable public address and radio support for the Depot.

b. The Director, Telephone Services, heads the Division. The Director exercises staff cognizance over the telephone services and public address systems.

c. The functions of the Division are critical to the successful operation of all voice communications for the Depot.

(1) Telephone Services Branch. The Telephone Services Branch installs, manages, and maintains the Depot telephone network. Other responsibilities include monitoring the telephone bill for unofficial

telephone calls. The Branch also is responsible for all acquisitions and implementation of base telephone assets.

(2) Public Address Branch. The Public Address Branch is responsible for all permanent and portable public address systems and radio assets for the Depot. The Branch also provides Maintenance Management procedures for the Department.

CHAPTER 2

ANCILLARY RESPONSIBILITIES

This page is intentionally left blank.

CHAPTER 2

ANCILLARY RESPONSIBILITIES

2000. GENERAL. The collateral and support functions discussed in this chapter play an integral role in sustaining the mission of CISD. The value of their contribution depends upon their conscientious application of time and effort in executing their specific responsibilities. These collateral and support functions are:

1. Information Systems Security Manager (ISSM)/Information Systems Security Officer (ISSO)

2. Communications Officer

3. End-user

4. RI/ISC

5. EUCE Program Manager

6. LAN Group Administrator

7. TASO

8. Command Support Responsibilities

2001. INFORMATION SYSTEMS SECURITY MANAGER/OFFICER. The DAA appoints the ISSM and ISSO. The ISSM acts as the focal point for, and is the principal advisor to, the DAA on all automated computer system security procedures, including personnel, physical security, communications, emanations, hardware, and software. The ISSO reports to the ISSM and is the field expert on security matters. A more detailed part of the ISSO duties are:

1. Authorized to suspend operations, partially or completely, immediately upon detection of activities that appear to compromise or jeopardize security. His/her authority shall allow suspension of support service privileges to any system terminal subscriber, regardless of subordination, not adhering to regulations and procedures in effect at that time.

2. Ensure effective implementation of applicable computer security operations.

3. Prepare, disseminate, and maintain plans, instructions, guidance and/or operating procedures required to ensure security of computer operations.

4. Ensure that a TASO is properly appointed for each activity to manage and control remote terminal operations.

5. Ensure that RI/ISC is properly appointed and trained.

2002. COMMUNICATIONS OFFICER. The Deputy Director of CISD is the Communications Officer and is responsible for:

1. Carrying out his or her duties as a special staff officer in accordance with FMFM 10-1.

2. Acting as the cognizant officer on communications matters that require action by the Command.

3. Advising the Director, CISD, on matters pertaining to communications support and the state of communications aboard the Depot.

4. Advising and assisting other officers in the continuing effort to improve communications security and practices aboard the Depot.

5. Overseeing routine and special communications operations within the command.

6. Developing, testing, and evaluating new communications procedures and system designs to improve efficiency and reduce costs.

7. Recommending improvements to existing Depot communications systems when appropriate.

8. Establishing a mission-oriented and MOS training program based on assigned mission and the amount of training required for each incumbent in order to satisfactorily contribute to the accomplishment of assigned tasks.

2003. END-USER. End-users are responsible for maintaining EUCE assets assigned to them in peak operating condition by doing the following first echelon maintenance tasks:

1. Properly identifying and configuring the hardware (system unit components, peripherals and devices.)

2. Properly configuring the software to match the hardware.

3. Properly diagnosing and resolving common computer problems.

4. Properly diagnosing and reporting unresolved computer problems to the Help Desk, as well as those problems that are not resolvable at the first echelon level.

5. Taking all precautions necessary to maintain security regulations in the use of the AIS, LAN, and Internet, to include the prevention of the introduction of microcomputer viruses into their systems.

6. Exploiting local available microcomputer training to become proficient in the use/operation of EUCE/applications.

2004. EUCE PROGRAM MANAGER. The Director, ISSD, is the EUCE Program Manager and is responsible for:

1. Maintaining an understanding of the marketplace and the types of automated hardware/software tools available.

2. Maintaining an awareness of the pitfalls in using EUCE technology.

3. Maintaining an understanding of how to incorporate EUCE technology into the organization and mission of the Depot.

4. Maintaining an understanding of how to measure the impact of EUCE technology on performance, and on the success and efficiency of organizational operations.

5. Maintaining an understanding of the role and responsibility of the EUCE user as compared to that of data processing professionals.

6. Maintaining a copy of all applicable DOD, Navy, Marine Corps, and Depot orders and directives.

7. Maintain a database of Depot EUCE for the purpose of providing EUCE support, including upgrades and redistribution of resources. This database will cover all microcomputers, associated peripherals, and software. Database information to be provided by the unit ISC will include the following information:

User (by T/O line number)	Make
Model	Serial number

The EUCE Program Manager will provide the Supply Chief, CISD, with information about any movement of EUCE for either relocation or destruction.

2005. RESPONSIBLE INDIVIDUAL/INFORMATION SYSTEMS COORDINATOR. The RI/ISC is a sergeant or above to include an officer, or civilian of equivalent grade nominated by the units Commanding Officer or a Staff Officer to preside over the utilization and security of office information systems (microcomputers and associated peripherals) assigned to his or her unit. The Director, CISD, appoints them after the nomination from his/her unit. Within his/her assigned area of primary responsibility, the RI/ISC shall:

1. Accept consignment of and maintain an accurate inventory of all EUCE hardware and software consigned to his/her custody.

2. Gain a working knowledge of the provisions of this Depot Order, which specifically applies to the execution of the duties of RI/ISC.

3. Implement the security policies and procedures prescribed by this Depot Order and as advised by the ISSM and ISSO.

4. Ensure that each person authorized to have access to the unit's computing assets can be identified and held accountable for their actions.

5. Indoctrinate all computer users about their security and control responsibilities as outlined in this Depot Order, to also ensure that all members of his/her unit attend the INFOSEC annual security training.

6. Ensure that data security countermeasures are in place and that data integrity is protected from such potential hazards as negligence, theft, and malicious destruction in accordance with the INFOSEC regulations.

7. Ensure that physical security countermeasures are in place and those computers and peripherals are protected from such potential hazards as

malicious destruction, theft, and adverse environment (e.g., exposure to rain, direct sunlight, high humidity, extreme heat, excessive foot traffic, etc.)

8. Conduct random, unannounced inspections of each government-owned personal computer (PC) and remove any unauthorized or illegal software. Inspections will be carried out at least once every quarter. If inspections result in the removal of mission-essential software from the PC, contact CISD for assistance on obtaining legal software.

9. Reconcile the unit's CISD Consolidated Memorandum Receipt (CMR) on a quarterly basis with the CISD Supply Department within the time prescribed by MCO 4400.150.

10. Report all security violations to the INFOSEC team in a timely manner.

11. Ensure that the user performs first echelon maintenance before calling the Help Desk for assistance.

12. Review EUCE requirements and initiate requests for new or upgraded computing assets and associated peripherals for his/her unit using the format in Appendix A, and be the point of contact for such requests.

13. Assist the EUCE Program Manager in collecting valid information to authenticate requirements for new or upgraded computing assets requested by the unit.

14. Notify the EUCE Program Manager of an impending transfer at least 30 days prior to leaving the unit.

15. Attend all ISC Meetings held by CISD to receive instruction and information about events, taskings, and policy and procedure changes. If unable to attend, to ensure a representative is present.

2006. TERMINAL AREA SECURITY OFFICER. The TASO is appointed by the Director, CISD, and as part of his/her duties is responsible for:

1. Reporting to the INFOSEC Team on security issues.

2. Ensuring that each terminal user's identity, need-to-know, and access authorizations are established commensurate with the functions required by the terminal user's occupation, to include the 3270 access regulations.

3. Managing the control and dissemination of user and system ID's and passwords.

4. Taking actions to assist the Depot INFOSEC team in ensuring overall system security.

2007. RECRUIT ACCOUNTABILITY SYSTEM/PERSONNEL ACCOUNTABILITY SYSTEM (RAS/PAS) ACCOUNT MANAGER. H&S Battalion S-3 and Recruit Training Regiment S-3 supports

Ras/Pas with database administrators, which are tasked with maintaining user accounts in RAS/PAS. There will be at most three personnel from each command assigned 'supervisory' access. These personnel will receive specialized training from CISD Programming & Processing. These personnel are then tasked with scheduling potential new users into monthly classes run by CISD. Upon successful completion of the class, the RAS/PAS Account Manager will create an account in the proper database with the proper access. He/she will then contact CISD Help Desk to give the customer access to the network drives and folders required.

2008. COMMAND SUPPORT RESPONSIBILITIES

1. General/CO and Special Staff Officers

a. Forward requests for EUCE to the Director, CISD, for evaluation using the format in Appendix A.

b. Provide required usage and funding data, as required, for economic evaluation.

c. Nominate, in writing, a RI/ISC for EUCE, with that nomination sent to the Director, CISD, using the format in Appendix C.

d. Require end-users demonstrate proficiency in computer operation and first echelon maintenance before they are allowed to use a computer.

2. AC/S, G-4

a. Account for all EUCE classified as Plant Property (acquisition cost of over $5,000.)

b. Coordinate maintenance of proprietary EUCE and associated peripheral equipment classified as Plant Property as requested by CISD.

3. AC/S, Comptroller. Ensure equipment needed/requested has been validated by CISD before funding purchases.

4. Director, Service and Supply Division

a. Review procurement packages for EUCE to ensure each meets the following criteria:

(1) Procurement of EUCE is approved by a feasibility study conducted by the CISD, and subject to funds availability.

(2) The designated 1A fund administrator from CISD signs procurement documents, specifically DD Form 1149. No other Depot units are authorized to prepare or process procurement documents for EUCE and associated peripherals, including software.

b. Notify CISD when new EUCE has been received, including make, model, serial number, location, warranty information, and purchase price.

c. Request service contracts for proprietary EUCE classified as Plant Property.

d. Account for all EUCE classified as minor property (acquisition cost of under $5,000.)

e. Request service contracts and coordinate maintenance of proprietary ADP equipment classified as minor property as requested by CISD.

f. Advise Supply Department, CISD of service contract provisions at the beginning of each new contract.

g. Notify the CISD and Accounting Division when new EUCE classified as minor property have been received, including make, model, serial number, location, warranty information, and purchase price.

5. Primary Control Point (PCP)

a. PCP Assignments. The following staff and special staff officer, commanding officers, and officers in charge are designated as PCPs and will receive a monthly toll call statement:

Commanding General/Staff Secretary
AC/S, G-1
AC/S, G-2/3
AC/S, G-4
AC/S, Comptroller
AC/S, QMD
AC/S, Recruiting
AC/S, Religious Ministries
AC/S, SJA
Director, CISD
CO, Recruit Training Regiment
CO, Support Battalion
CO, 1st RTBN
CO, 2nd RTBN
CO, 3rd RTBN
CO, H&S Battalion
CO, Headquarters Company
CO, Service Company
Manager, Recreation Branch, MCCS
Director, TVISC
Director, Human Resource Office
Director, Finance Office
Director, Family Services Center
Director, Food Services Division
Director, Facilities Division
Director, Recruiters School
Director, Service and Supply Division
Motor Transport Officer
Property Control Officer
Public Works Officer
PMO
PAO
Traffic Management Officer
Depot Adjutant
Manager, Food/Hospitality Branch, MCCS

b. PCP Responsibilities. The PCP is responsible for the following:

(1) The control of local area/long distance dialing in his or her unit. PCPs may reduce the monthly charges incurred by his or her unit by limiting or reducing the following:

(a) The number of instruments per office.

(b) The number of instruments with Class of Service (COS) other than COS 6.

(c) Establishing and enforcing local policies on telephone usage.

(2) The verification of official/non-official/non-verifiable telephone calls on the monthly unit toll call statement.

(3) Referring those found abusing telephone equipment/service to the Commanding Officer for disposition of offense(s) against the UCMJ.

(4) The appointment of a Telephone Control Officer (TCO) and providing a copy of the appointment letter to the Telephone Officer.

6. TCO. A PCP, using the format in Appendix D, may assign officers and SNCOs as the TCO. The TCO's primary function is to assist the PCP by executing the following tasks:

a. Verifying the status (official/non-official/non-verifiable) of each telephone charge on the monthly toll call statement.

b. Alerting the PCP to cases of telephone equipment/services abuse.

c. Correctly marking the monthly statement. The TCO will ensure that the monthly toll call statement is properly marked during the verification process. Instructions for marking the toll charge bill are as follows:

(1) Official calls will be marked "official."

(2) Non-official calls will be marked with the caller's rank and name in the right-hand margin.

(3) Unverifiable calls will be circled in red ink and will be referred to the Criminal Investigation Division for investigation.

d. Returning toll call statements and payments. Verified original toll call statements will be returned to the Telephone Officer within ten working days from date of receipt. The Director, CISD, may grant extensions, if valid justification is presented prior to the end of the ten-day period.

e. Identifying discrepancies on the toll call statement. The telephone statement will be reconciled with a telephone log. The TCO will alert the Telephone Officer to discrepancies on the monthly toll call statement as necessary. Discrepancies include, but are not limited to, the following: phone numbers not belonging to the TCO's unit, calls not made by the unit, and calls billed to the unit.

f. Notifying the Telephone Officer of an impending transfer at least 30 days prior to leaving the unit.

CISD SOP

CHAPTER 3

END USER COMPUTING EQUIPMENT (EUCE)

This page is intentionally left blank.

CHAPTER 3

END-USER COMPUTING EQUIPMENT (EUCE)

3000. GENERAL. EUCE is a comprehensive term used to designate all microcomputer assets including such auxiliary equipment as monitors, keyboards, printers, modems, all types of drives, soundboard, video board, computer speakers, computer driven audiovisual and communication systems, and software.

3001. ACQUISITION

1. Purpose. EUCE will only be acquired to reduce manpower needs and/or increase work performance. These benefits must fully justify the cost of the equipment and associated peripherals.

2. Funding. Personal computers, laptop computers and servers are centrally managed and procured with Procurement Marine Corps funding only.

3. Requests. All requests for EUCE will be submitted to CISD for a feasibility study using the format in Appendix A. The results of the study and a final recommendation will be forwarded with the original request, via chain of command, to the Chief of Staff.

4. Restrictions. To guarantee EUCE requested or required is compatible with the Depot's installed system, all EUCE procurement will be processed by CISD only. No other unit of the Depot is permitted to process its own EUCE procurement.

3002. LEASE ACTIONS. Procurement of microcomputers shall be accomplished based on lowest total overall cost (LTOC.) Since purchase normally represents the LTOC alternative, lease is only authorized when an economic analysis clearly shows that leases represent the LTOC approach over the system life of the requirement. The approval threshold for lease of equipment is to be based on the current purchase equivalent cost and must be approved by the Director, CISD, prior to entering any agreement.

3003. INVENTORY

1. Database. The EUCE Program Manager will maintain a database of Depot EUCE for the purpose of providing EUCE support, including upgrades and redistribution of resources. This database will cover all microcomputers, associated peripherals, and software.

2. Data Input. Inventory data shall be provided by the unit RI/ISC and will include the following information:

User (by T/O line number)
Description of the EUCE
Serial number
Manufacturer
Appropriated and nonappropriated funds
User billet nomenclature

3. Reconciliation. Inventory of all EUCE assigned to an unit's hand receipt shall be reconciled with the Supply Department's master database by the RI/ISC during the first month of each fiscal quarter in accordance with MCO 4400.150. During the reconciliation, all EUCE serial numbers and 'on

hand' quantities must be physically inventoried. Equipment cannot be removed from the database without proper justification. Equipment acquired during the quarter that does not appear on the unit CMR must be reported.

3004. EMPLOYMENT OF END USER COMPUTER EQUIPMENT

1. Use. All EUCE purchased by the Depot is intended for official use only. Care will be taken to ensure that the manufacturer's warranty requirements are followed.

2. Software Usage. All software purchased for the microcomputers will be used in strict compliance with licensing agreements. Proprietary software cannot be copied for distribution aboard the Depot for either personal or instructional purposes.

3. Inkjet Printers. Inkjet printers are encouraged since they are less expensive than laser quality printers. They have been approved for use for internal Marine Corps correspondence.

4. Supported Software. Supported software includes the Marine Corps primary and secondary standards.

a. The primary standard for an operating system is Microsoft Windows.

b. The primary application standard for word processing, database management system, presentation graphics, and spreadsheets is Microsoft Office.

c. All other software applications are non-standard and require a waiver from the office of C4I at HQMC.

d. Maintaining the original diskettes/CD's of any application programs issued to a unit is the responsibility of that unit's RI/ISC.

5. Nonsupported Software. Nonsupported software includes programs and packages not listed in paragraph 4, but granted a waiver for use by units requiring specialized software to accomplish their assigned tasks (e.g. AutoCad, Page Maker, Corel Draw, etc.). The ISSD Training Branch staff and the Help Desk staff will provide assistance where possible, but may not be familiar with the program.

6. Privately Owned Microcomputers and Software. The use of privately owned microcomputers for work in Depot offices is authorized subject to controls over records, property, and personnel. The privately owned microcomputers must be registered with the Depot INFOSEC team and receive a waiver from the Director, CISD, for usage aboard the Depot. Privately owned software may be used on privately owned systems only and must be registered.

a. Records created, used, stored, etc. on privately owned microcomputers for official work is the property of the government, subject to records management directives.

b. The Depot is not liable for loss, damage, theft, maintenance, or any repair of privately owned microcomputers or software.

c. Managers and supervisors will ensure that government files and records

created and used on privately owned microcomputers for Depot activities remain accessible to the government, regardless of whether the privately owned computer remains, is removed, becomes inoperable, etc.

d. Any privately owned microcomputer brought onboard the Depot is subject to search.

3005. SOFTWARE DEVELOPMENT

1. CISD

a. Federal Government, DoD, and/or public domain software shall be used wherever possible. In the event that this software is not available or local procedures cannot be modified to the extent needed to apply DoD/public domain software to meet the requirement, commercial off-the-shelf software (COTS) will be used. Only when neither of the two routes can provide software capable of supporting the user's needs will the development of special purpose software be undertaken. The development effort shall be closely coordinated between the end-user and the Director, CISD, to ensure that all necessary development criteria are met.

b. CISD will develop and support applications used or shared by two or more units or activities. For example:

(1) RAS/PAS. A system used by all units aboard the Depot for managing all accountability and training records. The requirement for shared access, centralized management, and mass imports precluded the use of COTS software.

(2) Substance Abuse Testing & Tracking. A system used throughout the Navy/Marine Corps for substance abuse sample management. No known application is available for streamlining this complex task.

(3) A financial system that allows AC/S, Comptroller management of budgetary allotments while providing checkbook management features for the local commands. No known system exists with the following features, 1) multi-user local checkbook management, 2) centrally managed funding allotment and 3) Class I system reconciliation. (Example of capability only)

(4) An inventory management system that interfaces with the financial system to simplify the inventory process aboard the Depot. No known system is available to track assets from purchase request (see above) through end of useful life. Must be able to interface with multiple Class I official USMC applications on both the finance and supply fields. (Example of capability only)

c. Requests must be directed to the Director, CISD, using MCRD Form 5230/37, Request for AIS Support.

2. End-user

a. Other than specified in paragraph 3006, all end-user applications will be developed by the end-user. Current Depot standard software (i.e. Microsoft Office) will be used when applicable. ISSD will provide training on Depot standard software, and will assist users by reviewing programs and recommending programming procedures and techniques.

b. Applications developed using software other than Depot standards (i.e.

WordPerfect, dBASE, Lotus, etc.) will not be supported.

c. CISD Programming & Processing in concert with the Functional Managers of a custom application are responsible for the creation and implementation of a training program for the use of that application.

3. Application Program Documentation

a. All application programs shall be documented. For end-user developed programs, the following minimum documentation is required:

(1) Statement of purpose/methodology.

(2) Database structure/application source.

(3) Point of contact information, name, unit, etc.

b. For network/Depot-developed programs, documentation will be in accordance with NAVDAC PUB 17.15 dated 1985 (NOTAL.)

c. Documentation shall be maintained at the originator's unit, with a copy forwarded to the Programming and Processing Division, CISD.

3006. MAKING COPIES OF SOFTWARE

1. Copyrighted Material. This is a licensed copy of a program to be used on a single computer. Copies can be made for backup purposes only. Certain copyrights or license agreements may not allow any copies.

2. Copy Protection. A number of programs come copy-protected; either backup copies cannot be made or only a minimum number of copies can be made. The copy protection shall not be disabled or otherwise by-passed.

3. End-user Responsibility. The making of copies of software shall be in compliance with copyright or license agreements. The use of "de-protection software" is not authorized. "Pirating" (making unauthorized copies of software) is a violation of copyright laws, and violators are subject to prosecution. Unauthorized copies are illegal even if they are used only for the government jobs and never taken home for personal use.

3007. PRIVATELY-OWNED SOFTWARE. The use of privately owned software on Marine Corps microcomputers is prohibited. However, it is authorized on privately owned microcomputers once the software is approved for use and the microcomputer is duly registered with CISD. However, the responsibility for the security and proper use of these computing assets rests with the owner. This command and CISD do not assume liability for the loss or destruction of privately owned hardware and software.

3008. LOCAL AREA NETWORK. Official copies of LAN versions of standard software packages listed in paragraph 4 of Section 3005 are authorized to reside on the LAN. Microcomputer applications developed by the CISD are also authorized to reside on the LAN. Official copies of stand-alone versions of standard software packages, as well as all other stand-alone non-authorized software or software packages are not authorized to reside on the LAN. If unauthorized software or software packages are discovered on the LAN, the Network Division will remove the unauthorized software.

CISD SOP

CHAPTER 4

SECURITY

This page is intentionally left blank.

CHAPTER 4

SECURITY

4000. BACKGROUND

1. Special security considerations apply to microcomputers over and above those that are applicable to users of mainframe computer systems. All data available on the mainframe system is considered to be available for official use by authorized users of the system. These conditions may exist within the microcomputer users area. With microcomputers, the total security responsibility is with the end-user.

2. There is a need to treat microcomputer systems differently because anyone can easily walk off with a diskette full of data or programs for use at home. Proper management of access controls and data storage is essential to data integrity and security. Sensitive information includes personal information subject to the Privacy Act of 1974, source selection information, etc.

4001. MINIMUM SECURITY. Minimum security requires the implementation of procedures for prevention of loss from natural hazards, fire, theft, and malicious acts. A normal office environment will usually provide suitable environmental controls for operational reliability. EUCE will be operated within the manufacturer's temperature and humidity range specifications. Protection against unauthorized access, theft, and malicious acts will be provided by security controls commensurate with the value of the hardware components and the physical environment. The method of locking is at the discretion of the unit RI/ISC.

4002. RI/ISC SECURITY RESPONSIBILITIES. Key components to the security of EUCE are that:

1. Office doors and windows are secured whenever the office space is vacant.

2. The original application software diskettes are not used regularly, unless required by the software licenses. If necessary, a working copy should be made and the originals secured in a lockable cabinet, etc., controlled by the RI/ISC.

3. All unit or office personnel are thoroughly familiar with and actively practice security/lock-up procedures established within the using unit by the RI/ISC.

4. Data backup procedures for locally created files and LAN files are established and routinely followed to ensure data and programming survivability.

5. During the initial boot of a microcomputer system, and before a user can perform any work, the following message will appear on the screen in a fashion that requires the user to take an overt action to clear the screen. The message will read as follows:

NOTICE AND CONSENT LOG-ON BANNER

> This is a DEPARTMENT OF DEFENSE COMPUTER SYSTEM. This computer system, including all related equipment, networks and network

devices (specifically including internet access), are provided only for AUTHORIZED U.S. GOVERNMENT USE. DoD Computer systems may be MONITORED for all lawful purposes, including to ensure that their USE IS AUTHORIZED, for management of the system, to facilitate protection against unauthorized access, and to verify Security procedures, survivability and operational security. Monitoring includes active attacks by authorized DoD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information, including personal information, placed on or sent over this system may be monitored.

Use of this DoD computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal or other adverse action. Use of this system constitutes CONSENT TO MONITORING for these purposes. (Reference: DoD General Counsel Memo, dtd 27 Mar 1997 applies)

Press "Y" to confirm consent

6. Supervision of the above requirements is constant.

4003. END-USER SECURITY RESPONSIBILITIES. End users are responsible for the security considerations of the hardware, software, and data. For example, information can be easily lost if the end-user does not back up files regularly with current copies of the data and any programs that have been revised. Valuable software and data can also be stolen. The following security measures are required:

1. Establish lock-up procedures for software packages and data file diskettes when not in use.

2. Original software diskettes shall be turned over to the RI/ISC after the application(s) have been installed.

3. Establish and use back-up procedures for locally created files.

4. Use microcomputers and software for official business only.

5. Do not permit unauthorized removal of hardware, data files, or software from the workstation.

6. No classified information will be entered into EUCE.

7. Processing of Privacy Act data or information will be in compliance with applicable regulations.

4004. PASSWORDS. Once physical security is ensured, the use of passwords is the primary means of data security. Passwords are assigned to individuals whose responsibility is to ensure that unauthorized personnel are not allowed access to their password(s).

4005. SOFTWARE VIRUSES

1. The introduction of microcomputer viruses, which often are the work of knowledgeable computer pranksters, are programs that can clone themselves rapidly, spreading from one microcomputer disk (floppy or hard) to another and one microcomputer program to another. The virus also can corrupt files or infect a LAN by duplicating itself into computer programs or operating system software. Viruses modify a program's operation, causing the computer to malfunction or crash. At their worst, they destroy vital data.

2. A microcomputer virus can be easily inserted into a program that is placed on a bulletin board as "freeware" and "shareware." A user can download the program into their microcomputer unaware that it contains a virus. In order to minimize or preclude this from happening to microcomputer users throughout the Depot, the following precautionary measures will be observed:

a. Use only microcomputer software that comes in factory-sealed containers from reputable dealers.

b. Do not download executable programs from bulletin boards or the Internet directly to a hard disk or onto a LAN.

c. Do not accept copied or pirated software. Observe copyright protection laws.

d. When possible, use a write/protect tab on diskettes.

e. Use only authorized microcomputer software provided through proper supply/requisitioning channels. No personal privately owned software is allowed without a waiver from the Director, CISD.

f. All software of questionable origin or quality will be brought to the ISSD Maintenance Section to be checked for viruses and license agreements before use.

g. All software downloaded from "public domain" software-sharing services (like bulletin boards, and the Internet) will be brought to the ISSD, CISD to be checked for viruses and license agreements before use.

h. Only software authorized by the Network Director or LAN Chief will be used on the network.

i. Run antivirus software continuously on all microcomputers.

CISD SOP

CHAPTER 5

CUSTOMER SUPPORT SERVICES

This page is intentionally left blank.

CHAPTER 5

CUSTOMER SUPPORT SERVICES

5000. GENERAL. CISD shall provide customer service support for Depot personnel. Customer service support discussed in this chapter shall be provided in a manner relevant to performance improvement, and without conditions or assumptions, the best in enabling the customer's successful execution of their assigned tasks.

5001. MAINTENANCE

1. The CISD will provide in-house maintenance on all non-proprietary EUCE. Proprietary equipment will be placed on a maintenance contract administered by the responsible activity.

2. For corrective or preventive maintenance on nonproprietary EUCE, contact the Help Desk (extension 4-1390), reporting the make, model, serial number, description of problem, and a point of contact (name, location, etc.).

3. The ISSD shall provide microcomputers and printers for temporary backup replacement when a Depot desktop microcomputer or printer is down for repairs for an extended period of time when possible.

5002. LAPTOP/NOTEBOOK TEMPORARY LOAN

1. The ISSD has portable microcomputers (laptops and notebooks) available for utilization by Depot personnel while on official trips, inspections, etc.

2. Requests for utilization of a portable microcomputer will be submitted to the Director, ISSD, CISD, identifying the requirements for a microcomputer, software required, and signed by a General/CO or Special Staff Officer, using the format in Appendix E.

5003. MICROCOMPUTER TRAINING PROGRAM. The basic purpose of the training program is to optimize the promised benefits from the massive investments made in hardware and software assets in improved performance, and to bring about the anticipated and necessary changes to improve business procedures. The objectives of the training courses will not only focus on competency in using the supported software programs, but also in developing proficiency in the effective use of these applications to accomplish assigned work.

1. Workcenter Manager Responsibility. To optimize the benefits of training, work center managers are required to do the following:

a. Schedule training after end-users have had the opportunity to become familiar with the hardware and software they will be working with.

b. Support the end-user's need to explore the hardware and software and practice new skills. Regulate workloads before and after training to allow for experimentation and reasonable rates of learning.

c. Pace post-training work assignments to help end-users strengthen their skills over time.

d. Urge end-users to broaden their skills and knowledge and create new uses for the technology.

2. End-user Responsibility

a. Set-up your working environment prior to the training. Make sure your hardware and software have been installed properly.

b. Explore your hardware and software. Become familiar with their basic look and feel on your own and with the help of tutorials.

c. Identify ways you will use the system before attending the training.

d. Plan your learning path. Talk to your manager or a training specialist to map out a training path including goals and objectives.

e. Participate actively in your training classes. Try to relate what you are learning to problems on the job.

f. Practice what you have learned. Begin using the software the day after training and schedule time for practice and/or regular use. Share your progress with your manager.

g. Expand your knowledge and skills. Keep looking for new and more challenging applications. Take intermediate or advanced training where offered to avoid leveling at the beginner level.

3. Training Classes. The ISSD will provide the training classes and the necessary equipment to carry out the prescribed training objectives.

4. Class Scheduling

a. Classes will be scheduled on a monthly basis, adjusted to the demand of microcomputer users and availability of resources.

b. Class size is limited to one student to each microcomputer. This requirement is to maintain hands-on time for all students and to avoid degrading the quality of training.

c. Special classes or block training for individual organizations are available for scheduling.

5. Request for Training

a. Training requests will be submitted by E-mail to training@mcrdsd.usmc.mil no later than five (5) working days prior to the scheduled convening date.

b. If the student is unable to attend a requested class, the requesting responsible authority should make every effort to find a qualified replacement and inform the Director, ISSD of the change. If a suitable replacement cannot be located, a letter requesting that the student be dropped from the requested training must be submitted no later than three (3) working days before the class convening date.

c. Special classes can be arranged if at least 100% of the classroom capacity can be utilized. Special classes can be given for courses specifically designed to meet the computing requirements of the unit.

5004. Local Area Network

1. Support. The CISD will provide in-house support on all government-owned PC's connected to the LAN by wire or by modem. Support is restricted to the Marine Corps Recruit Depot, San Diego, Weapons Field Training Battalion, Camp Pendleton, and the Marine Liaison at Balboa Naval Hospital. All requests for support must be submitted by calling the CISD Help Desk or via E-mail, if feasible.

2. Expansion. The CISD will provide both physical and administrative expansion of the LAN (i.e., installing additional LAN cabling or computers or adding additional users to a LAN Group). All requests for expansion must be submitted to the Director, CISD, either via E-mail or by completing Form MCRD 5230/37 (Rev. 9-89), Request for AIS Support.

3. Relocation. Users are prohibited from relocating LAN-connected EUCE. When relocation of EUCE is required, CISD will provide for the physical relocation of all LAN equipment and computers involved. All requests for relocation must be submitted to the Director, CISD, either by LAN or by completing Form MCRD 5230/37 (Rev. 9-89), Request for AIS Support.

4. Individual LAN Accounts

a. Naming Standards. The naming of all LAN accounts shall be in accordance with MCEN standards as set forth by the MITNOC, MCB Quantico, VA. Item Name- the Item name for an individual mailbox will be a user's rank, given name, middle initial and surname, all in capital letters. In cases where a person's surname ends in a title (Jr, Sr, II, III) or has a space (Van Doss, Smith Jones) the name must be bridged by an underscore. Only letters, numbers, spaces, decimal points, underscores, and dashes will be used.

Example: MAJ JOHN JONES, MAJ JOHN M JONES, and MAJ JOHN M JONES_JR

b. Individual LAN Account Names. The name of an individual's network account will be the user's surname and the first letters of the user's given and middle name. If an account with that name already exists, numbers will be added to the name to ensure the account name is unique within the network domain. All letters will be capital. Titles (Jr, Sr, II, III) will not be appended. If the surname a space (Van Doss, Smith Jones) the space will be removed in the account name. Only letters and numbers will be used.

Example: MAJ John M Jones III will be JONESJM or JONESJM2

c. Exchange Account Names. Microsoft Outlook/Exchange is the Marine Corps standard for E-mail. A separate account is required in Exchange to allow a LAN user to send and receive E-mail. All Exchange account names shall match the user's LAN account name. Additionally, other information such as given, middle and surname, rank, base, department, office, work address, telephone numbers shall be entered into the account. The display field information shall be entered in the following format: surname, rank, given name, middle name and title (II, Sr., Jr., etc.), if any.

5. Guidelines for Using Electronic Mail. The use of E-Mail has far reaching implications in the areas of information control and information security. Improper use of E-Mail can compromise sensitive information currently managed in accordance with Marine Corps records management directives. Adherence to the following guidelines offers significant protection against those

vulnerabilities. The Depot LAN is cleared for sensitive unclassified traffic only. The use of E-mail to send classified information is strictly prohibited.

a. E-Mail. E-Mail is restricted to official use only, as in the use of Government telephone and postal systems. To help in deciding if an electronic message is appropriate, ask the following questions before sending the message:

(1) Is it necessary in the performance of your job or beneficial to the health, welfare, or safety of others?

(2) Is the information presented in such a way that it will not embarrass an individual or the United States Marine Corps?

(3) Are you willing to share the contents of this E-Mail with others?

If you can answer yes to all these questions, then the E-Mail message is appropriate and can be sent.

b. Depot Wide Mail

(1) The only personnel allowed to send Depot wide messages are Help Desk personnel, LAN administrators, and the Depot Public Affairs Office (PAO).

(2) Message should be as brief as possible, no more than two or three sentences.

(3) If the message does not follow these parameters, then the information should be placed on the MCRDSD Public Folders, with a brief message going out to the Depot as to the location where the information can be found.

(4) Messages that are to be sent out Depot wide should be addressed to OMB PAO MCRD San Diego or ombpao@mcrdsd.usmc.mil. PAO personnel will review the message to ensure it meets the above criteria. If the message satisfies the requirements, it will be sent as part of the MCRD Daily News E-mail.

(5) Any personnel, other than those named above, sending a Depot-wide message will have their mail privileges revoked and may face disciplinary actions.

c. Policy On the Distribution of Announcements Via the Depot LAN. The distribution of official and unofficial announcements using the Depot LAN is encouraged because of the speed of delivery, the control of longevity of the message, and the low cost incurred. However, the very flexibility of the medium can be disruptive and counter-productive if not used in a controlled manner. The instructions on the methods and restrictions for electronic distribution will ensure the widest coverage with the least impact on operations.

(1) The LAN E-Mail system will only be used for Depot-wide announcements for critical, unplanned events that will occur within 24 hours and can cause either a serious disruption of Depot operations or present a potential for danger to property or personnel.

(2) Announcements that are to be sent out as Depot wide should be addressed to pao@mcrdsd.usmc.mil. PAO personnel will review each message to ensure it meets the above criteria. If the message satisfies the requirements, PAO personnel will send the announcement Depot wide to ensure proper distribution.

(3) If the subject does not pertain to the Depot, the E-Mail announcement will be sent using standard addressing or pre-existing mailing lists. Mailing lists shall be used whenever possible.

5005. MCRDSD PUBLIC FILES. The MCRDSD Public Files System is an element of the Microsoft Outlook/Exchange E-mail system that has been customized to provide a means of posting and maintaining long-term announcements, directives, and schedules. Each department/division will maintain its own folder(s) internal to the Public Folders and will appoint a folder supervisor for the day-to-day operations. CISD will be responsible for the overall operation of the Public Folders and its associated equipment. The MCRDSD Public Folders are made up of a number of specialty folders dedicated to a specific area, such as command schedules, and Executive Information System.

1. Maintenance. The Director, Network Division will provide in-house and maintenance control of the MCRDSD Public Folders.

2. Specialty Folders. Specialty folders are dedicated to a specific subject or command function. A folder supervisor will be assigned to each folder to be responsible for its content and structure, and for defining specific access rights for each folder. Specialty boards are dedicated to a specific subject or command function. A board supervisor will be assigned to each board to be responsible for its content and structure, and for defining specific access rights for each board.

3. Sections Folder. The Sections folder area is to be used to report status and standing for each of the sections listed in it. Each section will assign a folder supervisor to take charge of its own folder and supervise its structure and content, and to control its access and use.

4. Other Specialty Folders. Commanders and staff officers may open their own boards specializing in specific subjects, such as Announcements or Bulletins, or such command functions as G-1 schedule. The commander or staff officer must assign a folder supervisor for each folder they wish to open.

5. Usage. The MCRDSD Public Folders is primarily an open system. LAN users can access most areas of the folders to read, print, or download messages, and calendars. Most information stored in Public Folders is public and not controlled or secured.

6. Special purpose and controlled-access boards can be created. However, it is the responsibility of the Folder Supervisor to maintain and update the access list for those folders. No classified information can be posted on the MCRDSD Public Folders system.

5006. COMMUNICATIONS SUPPORT. Telephone Division provides equipment and services for routine and special requirements on and off the Depot. The most often requested forms of communications support include public address systems, inter-communications systems, and mobile radio systems.

1. Types of Communications Support

a. Basic Systems. Portable public address systems are kept on hand at the Telephone Division, and are available on a temporary loan/sub-custody basis, including the following:

(1) Public Address Systems. Systems are designed and implemented by the Telecommunications Branch at the request of the user.

(2) Radio Systems. Short range, hand-held radios are provided by the Telephone Branch.

(3) Paging Systems. Telephone paging devices (pagers) are provided by the Telephone Branch.

b. Complex Systems. Inter-communications systems and other design/planning intensive communications systems can be ordered for the requesting organization after a fiscal/maintenance support review is completed.

2. Requesting Communications Support

a. Requests for communications systems to support events occurring aboard MCRD shall be submitted to the Director, Telecommunications Division at least 72 hours prior to the desired date, or when stated in a Letter of Instruction.

b. Requests for design/installation, modification, or move of a permanently installed sound system shall be submitted to the Director, CISD.

5007. TELEPHONE SUPPORT. The Telephone Support Division provides the Depot telephone services in coordination with the appropriate telephone service vendor through the Navy Public Works Center.

1. Consolidated Area Telephone System-San Diego (CATO-SD). On 7 July 1988, MCRD became a user of the CATO-SD, a telephone system driven by an AT&T System 85 telephone switch. MCRD San Diego and Fleet Anti-Submarine Warfare Center Pacific make up the body of the North Military Complex, which is served by a single switch remote. The Navy's Consolidated Area Telephone Office is the interface between the telecommunications vendors and all bases using the CATO-SD system, as well as being the Depot's single point of contact for telephone service. CISD is the Depot's single point of contact for telephone service.

2. Types of Telephone Service. Each telephone installed/maintained by the federal government aboard the Depot for the purpose of conducting government business is assigned a specific COS. Each COS defines the limits of a telephone's capabilities.

a. Basic Class of Service. The following are the six basic COS available to users aboard the Depot.

COS 1 Provides long distance and priority DSN capability. (Note: the CATO-SD system is capable of providing this service to only one percent of the subscribers it serves.)

COS 2 Provides access long distance and Route DSN.

COS 3 Provides access to 619 area code calling Routine DSN.

COS 4 Provides access to long distance and local calling.

COS 5 Provides access to local calling.

COS 6 Provides base-to-base calling only.

b. Restrictions

(1) COS 1 - COS 3 telephones are the only telephones that may initiate DSN calls; all telephones within the CATS-SD system may receive DSN calls.

(2) Overseas DSN calls are placed through the DSN operator at (4-0400). Overseas DSN to include Hawaii, require a DSN Control number. This number is maintained by the unit's TCO. Without the control number the operator will not place the call.

(3) Calls of all DSN users/subscribers are subject to be pre-empted by calls of high precedence. A steady, high-pitched audible tone will indicate that the currently used circuit has been pre-empted.

3. Obtaining Telephone Service

a. Telephone Service Request (TSR). Government telephone service is obtained by submitting a TSR (see Appendix L) to the Director, Telephone Support Division. The following lists services provided and the time normally required to complete the TSR. TSRs disapproved will be returned via the chain of command specifying the reason(s) for disapproval, normally within five working days.

Service	TSR Completed (approximately)
*Telephone install/new phone	8 weeks
*Telephone relocation	8 weeks
Telephone removal	2 weeks
Change telephone number	1 week
Change COS	1 week
Add/remove features on/from a Telephone instrument	1 week

- The expense for relocating/re-installing telephones is prohibitively high; therefore, requests for such work on telephones installed within the previous 12 months shall be approved only when the requesting unit fully justifies and funds for the service.

b. Residential Telephone Service. A request for residential telephone service does not require the approval of CISD; the requesting Marine shall contact Pacific Bell directly at 811-5222 during the hours of 0830-1700, Monday through Friday.

c. Pay Telephone Service. Requests for pay telephone installation, relocation, or removal shall be coordinated through the Navy Recreation Services (NAVRECSVC). The MCRD San Diego NAVRECSVC Officer is the Facilities and Maintenance Telecommunications Manager of the AC/S, Marine Corps Community Services (MCCS) Office and can be reached at 4-4440. Responsibility for all pay telephone services belongs to AC/S MCCS.

d. Telephone Directories

(1) The Command Directory is published and distributed by the Telephone Support Division. Corrections or questions concerning this directory shall be directed to the Director, Telephone Support Division.

(2) The Pacific Bell White and Yellow Pages Directory for San Diego are published annually. One copy of White and one copy of Yellow Pages shall be made available to those offices that have local dialing capability.

e. Telephone Trouble/Repair

(1) Government telephone troubles shall be reported to the CISD Helpdesk at 524-1390.

4. Missing/Stolen/Physically Abused Telephone Equipment. Units with missing, stolen, or physically abused telephone equipment will have service restored upon submitting the following documents to the Director, CISD, via the chain of command.

a. A TSR for new instruments/equipment.

b. A copy of the Military Police blotter showing the reported loss, signed by the unit's commanding officer.

5. Use of Depot Telephones for Personal Calls

a. General. SECNAVINST 5370.2 restricts all DON military and civilian personnel from using government property, including government telephones, for anything other than official business or purposes. ALNAV 158/89 defines the criteria under which a local or long distance personal call is considered official business.

b. Policy

(1) Use of the Depot telephone system is limited to calls for official business, and those personal calls authorized below. No call other that these may be made even if it is the individual's intention to reimburse the government for the cost of the call.

(2) The Depot recognizes that both military and civilian employee's interest are best served by permitting employee's use of Depot telephones to conduct a modest amount of personal business, provided these calls do not incur a cost to the government. This means that for a personal call, a person must either:

(a) be calling a toll free number

(b) call collect, or

(c) use a calling card

c. Collections

(1) Individuals will be permitted to pay for any unauthorized calls. Reimbursing the government for unauthorized calls does not exempt the individual from appropriate administrative, civil, criminal, or disciplinary action.

(2) Reimbursement will include:

(a) The value of the call, based on the telephone usage report issued by the Communications Officer, plus three percent tax.

(b) A ten-dollar collection fee.

APPENDIX A

PRESCRIBED FORMAT FOR REQUESTING END USER COMPUTING EQUIPMENT (EUCE)

5230

From: RI/ISC (name, rank, and unit)
To: Director, Communications and Information Systems Department
Via: (Cognizant CO or Special Staff Officer)

Subj: REQUEST FOR END USER COMPUTING EQUIPMENT (EUCE)

1. Objective. Describe the objective you want to accomplish. This should be a general statement indicating the scope and complexity of the work to be done.

2. Current System. Describe the systems you are currently using. This description should include:

a. What kind of work is being done and what is the final finished product.

b. Present EUC assets including software.

c. What methods or procedures are involved in accomplishing the task(s).

d. What work or product(s) can be automated but are not because of insufficient EUC assets.

3. Proposed System. Describe the system you would like to see installed. This description should include:

a. How many and what type(s) of computing assets needed to accomplish your objective.

b. How you propose to use the computing assets requested.

c. Other information you feel would assist you in accomplishing your objective.

4. Productivity Enhancements and/or Costs. Describe how the additional computing assets would improve productivity. Include your estimates of manpower, material, or equipment savings. Give hard numbers.

5. Funding Available. Indicate whether funding is available from your own cost center. Also, provide a point of contact and telephone number.

Signature of RI/IS

Copy to:
EUCE Program Manager

APPENDIX B

PRESCRIBED FORMAT FOR NOMINATION OF UNIT
RESPONSIBLE INDIVIDUAL (RI)/INFORMATION SYSTEMS COORDINATOR (ISC)

UNIT HEADING

4400

From: Appropriate Nominating Authority
To: Director, Communications and Information System Department

Subj: NOMINATION OF ***(INSERT PERSONS FULL NAME)*** AS RESPONSIBLE INDIVIDUAL (RI) /INFORMATION SYSTEMS COORDINATOR (ISC) FOR ACCOUNT _____.

Ref: (a) SECNAVINST 5239.3
(b) OPNAVINST 5239.2
(c) NAVSO P5239-07
(d) MCO P4400.150D
(e) UM 4400.124
(f) DepO P4400.7C

1. Per the references, the following individual is hereby nominated as the new Responsible Individual and will also act as the Information Systems Coordinator (ISC) for account _____.

Name:_____

Rank:_____SSN:_____

Estimated Rotation Date:_____

Work Number:_____

Complete LAN Address:_____

Unit Area of Responsibility:_____
This should include building numbers & room numbers where more than one RI/ISC is present in the building.)

2. The effective date for this appointment is_____.

_____
/s/ I. M. AUTHORIZED

APPENDIX C

PRESCRIBED FORMAT FOR LETTER OF APPOINTMENT TO TELEPHONE CONTROL OFFICER

5230

From: (Appointing Authority)
To: Commanding General, MCRD, San Diego, California
(Attn: Director, Communications and Information Systems Department)

Subj: APPOINTMENT OF TELEPHONE CONTROL OFFICER

Ref: (a) DepO P5230.3D

1. In compliance with the reference, the following officer is assigned as the Telephone Control Officer for (name of unit).

Rank	Name	SSN

(Signature of Appointing Authority)

APPENDIX D

PRESCRIBED FORMAT FOR REQUESTING
TEMPORARY LOAN OF LAPTOP/NOTEBOOK COMPUTERS

5230

From: (General/CO or Special Staff Officer)
To: Director, Information Systems Support Division

Subj: TEMPORARY LOAN OF A PORTABLE LAPTOP/NOTEBOOK

Ref: (a) DepO P5230.3D

1. I request that a portable Laptop or Notebook be made available during the following period: _____ to _____ (not to exceed seven (7) days). This request meets the requirements of the reference and will be used for:

_____

2. The location of the Laptop/Notebook will be:

_____

3. **I understand that I will solely be responsible for the requested equipment.**

4. Point of contact: Name _____
Rank/Title _____
Ext # _____

_____
(Signature)

.....

FIRST ENDORSEMENT

From: Director, MicroComputer Repair Branch
To: (Requester)

1. Your request is: Approved / Disapproved.

You will be temporarily issued: one (1) Laptop or Notebook.

Number: _____
Make: _____
Model: _____

_____
(Signature)

APPENDIX E

TELEPHONE SERVICE REQUEST			
Using Unit	Bldg No.	Room No.	Date
Point of Contact for Detailed Information			Phone

Service Requested: (Check as many boxes as applicable)
(Relocations and Installations require a present and proposed diagram)

☐ Install ☐ Relocate ☐ Disconnect ☐ Call Pickup

☐ COS Change ☐ Call Coverage ☐ Intercom ☐ Abv Dialing

Classification of Service (COS):

☐ COS2 (Commercial and Conus DSN) ☐ COS4 (Commercial)

☐ COS3 (Commercial (619) and DSN) ☐ COS5 (San Diego area)

☐ COS16 (DSN and Base Only) ☐ COS6 (On Base Only)

Justification (How this request would save time and money)

Description (Work to be completed)

Do you want this number published? ☐ Yes ☐ No

Under which title would you like the new phone number listed in the directory?

Signature of Commanding Officer or Telephone Control Officer/Date

MCRD 2000/2 (Rev. 8-94)